Canad. J. Math. Vol. **69** (3), 2017 pp. 579–594
http://dx.doi.org/10.4153/CJM-2016-038-2
©Canadian Mathematical Society 2016

Regulators of an Infinite Family of the Simplest Quartic Function Fields

Jungyun Lee and Yoonjin Lee

Abstract. We explicitly find regulators of an infinite family $\{L_m\}$ of the simplest quartic function fields with a parameter m in a polynomial ring $\mathbb{F}_q[t]$, where $\mathbb{F}_q$ is the finite field of order q with odd characteristic. In fact, this infinite family of the simplest quartic function fields are subfields of maximal real subfields of cyclotomic function fields having the same conductors. We obtain a lower bound on the class numbers of the family $\{L_m\}$ and some result on the divisibility of the divisor class numbers of cyclotomic function fields that contain $\{L_m\}$ as their subfields. Furthermore, we find an explicit criterion for the characterization of splitting types of all the primes of the rational function field $\mathbb{F}_q(t)$ in $\{L_m\}$.

1 Introduction

Gras [4,5], Lehmer [13], and Shen [19] found families of monic irreducible polynomials with integral coefficients and constant term one whose Gaussian periods have degree 3, 4, 5, 6, and 8, respectively; these polynomials are called the *simplest* cubic, quartic, quintic, sextic and octic polynomials, respectively. Lazarus [11], Louboutin [15], and Washington [22] studied a family of simplest quartic number fields. They were interested in finding regulators and class numbers of the family of simplest quartic number fields, and they found simplest quartic number fields with small class numbers. In the case of function fields, Bae [1] and Feng and Hu [3] obtained the criteria for class numbers one or two for some family of quadratic function fields, and they found all quadratic function fields in the family with class numbers one or two. Moreover, Wu and Scheidler [24] considered a quartic function field K that is biquadratic, and they characterized splitting types of all the rational places in K and found their invariants such as genus, integral basis, and discriminant.

Let $k = \mathbb{F}_q(t)$ be a rational function field, where $\mathbb{F}_q$ is the finite field of order q with odd characteristic. We study an infinite family $\{L_m\}$ of *cyclic quartic function fields* given by $L_m = k(\alpha_m)$, where α_m is a root of $x^4 - mx^3 - 6x^2 + mx + 1$ and m is a monic polynomial in $\mathbb{F}_q[t]$ such that $m^2 + 16$ is square free in $\mathbb{F}_q[t]$.

We explicitly find regulators of an infinite family $\{L_m\}$ of the simplest quartic function fields with a parameter m in a polynomial ring $\mathbb{F}_q[t]$, where $\mathbb{F}_q$ is the finite field

Received by the editors October 14, 2015; revised October 5, 2016.
Published electronically December 6, 2016.
The authors were supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2009-0093827). Author J. L. was also supported by a National Research Foundation of Korea (NRF) grant founded by the Korea government (2011-0023688). Author Y. L. is the corresponding author and supported by a National Research Foundation of Korea (NRF) grant founded by the Korea government (MEST)(2014-002731).
AMS subject classification: **11R29**, 11R58.
Keywords: regulator, function field, quartic extension, class number.

https://doi.org/10.4153/CJM-2016-038-2 Published online by Cambridge University Press

of order q with odd characteristic (Theorem 1.1). In fact, this infinite family of the simplest quartic function fields are subfields of maximal real subfields of cyclotomic function fields with the same conductors. In fact, computation of regulators can make some contribution to finding class numbers of the family $\{L_m\}$. We obtain a lower bound on the class numbers of the family $\{L_m\}$ (Section 6) and some result on the divisibility of the divisor class numbers of cyclotomic function fields which contain $\{L_m\}$ as their subfields (Section 8). We find all the cyclic quartic function fields in the family $\{L_m\}$ whose class numbers are less than or equal to 20 with the positive degree of m (Table 3). Furthermore, we find an explicit criterion for the characterization of splitting types of all the primes of k in $\{L_m\}$ (Theorem 7.2); this is very useful due to its important role in computing the class numbers of L_m and zeros of zeta functions of L_m as mentioned in [17].

Our main result is the following theorem.

Theorem 1.1 *Let m be a monic polynomial in $\mathbb{F}_q[t]$ such that m^2+16 is square free in $\mathbb{F}_q[t]$. Then the regulator $R(L_m)$ of L_m is a factor of $2(\deg m)^3$ and*

$$R(L_m) \geq \frac{1}{2}(\deg m)^3.$$

Moreover, if $\deg(m)$ is an odd prime or $q \equiv 3 \pmod 4$, then the regulator of L_m is explicitly given by $R(L_m) = (\deg m)^3$.

Table 1 and Table 2 in the appendix present some lists of m and q satisfying our conditions to determine $R(L_m)$. We prove the existence of an infinite family $\{L_m\}$ satisfying the conditions of Theorem 1.1 in Section 5. Moreover, we determine all q and m for which the class numbers of L_m in the family are less than or equal to 20 in Section 6. The same types of quartic fields are discussed for the number field case in [11,15]. There is a significant difference between the number field case and the function field case in determining the index $Q_{L_m} := [U(L_m) : U(K_m)U(L_m/K_m)]$, where K_m is the unique intermediate quadratic subfield of L_m/k, $U(L_m)$ (respectively, $U(K_m)$) is the unit group of the maximal order of L_m (respectively, K_m), and

$$U(L_m/K_m) := \{\epsilon \in U(L_m) \mid N_{L_m/K_m}(\epsilon) = \epsilon\sigma^2(\epsilon) \in \mathbb{F}_q^*\}.$$

2 Preliminary

Let $k = \mathbb{F}_q(t)$ and let $L_m = k(\alpha_m)$ be a quartic extension of k that is generated by a root α_m of $x^4 - mx^3 - 6x^2 + mx + 1$, where m is a monic polynomial in $\mathbb{F}_q[t]$ such that m^2+16 is square free in $\mathbb{F}_q[t]$. Then the unique intermediate quadratic subfield K_m of L_m/k is in fact $k(\sqrt{m^2+16})$. It is known that L_m is a cyclic extension of k such that $\mathrm{Gal}(L_m/k) = \langle\sigma\rangle$ and $\mathrm{Gal}(L_m/K_m) = \langle\sigma^2\rangle$, where

$$\sigma(\alpha_m) = \frac{\alpha_m - 1}{\alpha_m + 1}.$$

Let $U(L_m)$ (respectively, $U(K_m)$) be the maximal order of L_m (respectively, K_m) as before. Let $U(L_m/K_m) := \{\epsilon \in U(L_m) \mid N_{L_m/K_m}(\epsilon) = \epsilon\sigma^2(\epsilon) \in \mathbb{F}_q^*\}$. It is known [4]

https://doi.org/10.4153/CJM-2016-038-2 Published online by Cambridge University Press

that there is $\eta_m \in L_m$ such that $U(L_m/K_m) = \mathbb{F}_q^* \times \langle \eta_m, \sigma(\eta_m)\rangle$, and we call η_m a *relative fundamental unit* of L_m over K_m.

The *infinite prime* $\wp_\infty$ of k splits completely in L_m. Therefore, there are four embeddings of L_m into $k_\infty = \mathbb{F}_q((t^{-1}))$ associated with the infinite primes $\mathfrak{P}_i$ of L_m lying over $\wp_\infty$ with $i = 1,2,3,4$, where k_∞ denotes the completion of k at $\wp_\infty$. We fix one of the embeddings associated with $\mathfrak{P}_1$ to define the degree of an element of L_m throughout this paper. For a nonzero element $a = \sum_{i=-m}^{\infty} c_i t^{-i} \in k_\infty$, where $m \in \mathbb{Z}$, $c_i \in \mathbb{F}_q (i \geq -m)$, and $c_{-m} \neq 0$, we have the valuation $v_{\wp_\infty}(a) = -m$, so we define the degree of a to be $\deg a = m$. Let $R(L_m)$ (respectively, $R(K_m)$) denote the regulator of L_m (respectively, the regulator of K_m) and for $\epsilon_i \in U(L_m)$ $(i = 1,2,3)$,

$$\mathcal{R}(\epsilon_1, \epsilon_2, \epsilon_3) := \begin{pmatrix} \deg \epsilon_1 & \deg \epsilon_2 & \deg \sigma(\epsilon_3) \\ \deg \sigma(\epsilon_1) & \deg \sigma(\epsilon_2) & \deg \sigma^2(\epsilon_3) \\ \deg \sigma^2(\epsilon_1) & \deg \sigma^2(\epsilon_2) & \deg \sigma^3(\epsilon_3). \end{pmatrix}$$

Throughout this paper let D_{L_m/K_m} (respectively, $D_{L_m/k}$) be the discriminant of L_m over K_m (respectively, L_m over k).

3 Determination of Relative Regulators

In this section we show that the relative fundamental unit η_m of L_m over K_m is equal to a root α_m of $x^4 - mx^3 - 6x^2 + mx + 1$ up to a constant in $\mathbb{F}_q^*$, under one of the following two conditions:

- $\deg(m)$ is an odd prime,
- $q \equiv 3 \pmod 4$.

It is known [4] that $Q_{L_m} := [U(L_m) : U(K_m)U(L_m/K_m)]$ equals 1 or 2 and

$$\mathcal{R}(\epsilon_{K_m}, \eta_m, \sigma(\eta_m)) = Q_{L_m} R(L_m).$$

Thus, for a determination of $R(L_m)$ and the relative fundamental unit η_m, we need a lower bound and an upper bound of $\mathcal{R}(\epsilon_m, \eta_m, \sigma(\eta_m))$. We note that for $\alpha \in U(L_m/K_m)$ and $\beta \in U(K_m)$, we have

$$R(\beta, \alpha, \sigma(\alpha)) = 2\deg(\beta)\big((\deg \alpha)^2 + (\deg \sigma(\alpha))^2\big).$$

Proposition 3.1 *Let $\eta_m \in L_m$ and $\epsilon_m \in K_m$ such that $U(L_m/K_m) = \mathbb{F}_q^* \times \langle \eta_m, \sigma(\eta_m)\rangle$ and $U(K_m) = \mathbb{F}_q^* \times \langle \epsilon_m \rangle$. Then we have $(\deg m)^3 \leq \mathcal{R}(\epsilon_m, \eta_m, \sigma(\eta_m)) \leq 2(\deg m)^3$.*

Proof Since $\alpha_m \in U(L_m/K_m)$, we have

$$\mathcal{R}(\epsilon_m, \eta_m, \sigma(\eta_m)) \leq \mathcal{R}(\epsilon_m, \alpha_m, \sigma(\alpha_m)) = 2\deg(\epsilon_m)\big((\deg \alpha_m)^2 + (\deg \sigma(\alpha_m))^2\big).$$

We note that $\alpha_m = m + \frac{5}{m} + \cdots$, $\sigma(\alpha_m) = 1 + \frac{5}{m} + \cdots$, and $\epsilon_m = m + \sqrt{m^2 + 16} = 2m + \cdots$ (see [3, proof Theorem 4.1]). Thus, we have $\deg \epsilon_m = \deg m$, $\deg \alpha_m = \deg m$, and $\deg \sigma(\alpha_m) = 0$. Finally, we obtain that

$$\mathcal{R}(\epsilon_m, \eta_m, \sigma(\eta_m)) \leq 2 \deg \epsilon_m \big((\deg \alpha_m)^2 + (\deg \sigma(\alpha_m))^2\big) = 2(\deg m)^3.$$

Now we note that $D_{L_m} = N_{K_m/k}(D_{L_m/K_m}) D_{K_m}^2 = (m^2 + 16)^3$. Since $D_{K_m} = m^2 + 16$, we note that $N_{K_m/k}(D_{L_m/K_m}) = m^2 + 16$. Moreover, D_{L_m/K_m} divides $(\eta_m - \sigma^2(\eta_m))^2$ in

https://doi.org/10.4153/CJM-2016-038-2 Published online by Cambridge University Press

K_m. Thus (m^2+16) divides $(\eta_m - \sigma^2(\eta_m))^2(\sigma(\eta_m) - \sigma^3(\eta_m))^2$ in k. Since $\sigma^2(\eta_m) = 1/\eta_m$ and $\sigma^3(\eta_m) = 1/\sigma(\eta_m)$, we have

$$\deg(m^2+16) \le 2|\deg \eta_m| + 2|\deg \sigma(\eta_m)| \le 2\sqrt{2}((\deg \eta_m)^2 + (\deg \sigma(\eta_m))^2)^{\frac{1}{2}};$$

this is because $a+b \le \sqrt{2(a^2+b^2)}$ for positive numbers a, b. It thus follows that $(\deg(m^2+16))^2 \le 8((\deg \eta_m)^2 + (\deg \sigma(\eta_m))^2)$. ■

3.1 Determination I

In this section, we determine a relative fundamental unit of L_m over K_m under the first condition that $\deg(m)$ is an odd prime.

Theorem 3.2 *If $\deg(m)$ is an odd prime, then α_m is a relative fundamental unit of L_m over K_m up to a constant in $\mathbb{F}_q^*$.*

Proof We note that

$$Q_{L_m} R(L_m) = \mathcal{R}(\epsilon_{K_m}, \eta_m, \sigma(\eta_m)) \mid \mathcal{R}(\epsilon_{K_m}, \alpha_m, \sigma(\alpha_m)) = 2(\deg m)^3$$

and $(\deg m)^3 \le \mathcal{R}(\epsilon_{K_m}, \eta_m, \sigma(\eta_m)) = Q_{L_m} R(L_m) \le 2(\deg m)^3$.

If $Q_{L_m} = 2$, we have $R(L_m) \mid (\deg m)^3$ and $1/2(\deg m)^3 \le R(L_m) \le (\deg m)^3$. If $\deg m$ is an odd prime, then we have $R(L_m) = (\deg m)^3$ and

$$\mathcal{R}(\epsilon_{K_m}, \eta_m, \sigma(\eta_m)) = \mathcal{R}(\epsilon_{K_m}, \alpha_m, \sigma(\alpha_m)) = 2(\deg m)^3.$$

If $Q_{L_m} = 1$, then $R(L_m) = \mathcal{R}(\epsilon_{K_m}, \eta_m, \sigma(\eta_m))$. We note that $R(L_m)$ is an even integer since $\mathcal{R}(\epsilon_{K_m}, \eta_m, \sigma(\eta_m))$ is an even integer. Let $R'(L_m) := R(L_m)/2$. Since $R(L_m) \mid 2(\deg m)^3$ and $(\deg(m))^3 \le R(L_m) \le 2(\deg m)^3$, we have

$$R'(L_m) \mid (\deg m)^3$$

and $1/2(\deg(m))^3 \le R'(L_m) \le (\deg m)^3$. If $\deg(m)$ is an odd prime, then we have $R'(L_m) = (\deg m)^3$ and $\mathcal{R}(\epsilon_{K_m}, \eta_m, \sigma(\eta_m)) = \mathcal{R}(\epsilon_{K_m}, \alpha_m, \sigma(\alpha_m)) = 2(\deg m)^3$. Since $\alpha_m \in U(L_m/K_m)$, we have $\alpha_m = c\eta_m^a \sigma(\eta_m)^b$ for $a, b \in \mathbb{Z}$ and $c \in \mathbb{F}_q^*$. We have $\mathcal{R}(\epsilon_{K_m}, \alpha_m, \sigma(\alpha_m)) = (a^2+b^2)\mathcal{R}(\epsilon_{K_m}, \eta_m, \sigma(\eta_m))$. Hence $\mathcal{R}(\epsilon_{K_m}, \eta_m, \sigma(\eta_m)) = \mathcal{R}(\epsilon_{K_m}, \alpha_m, \sigma(\alpha_m))$ implies that $\alpha_m = c\eta_m^{\pm 1}$ or $c\sigma(\eta_m)^{\pm 1}$; this implies that α_m is a relative fundamental unit up to constant in $\mathbb{F}_q^*$. ■

3.2 Determination II

In this section, we determine a relative fundamental unit of L_m over K_m under the second condition that $q \equiv 3 \pmod 4$.

Theorem 3.3 *If $q \equiv 3 \pmod 4$, then α_m is a relative fundamental unit of L_m over K_m up to a constant in $\mathbb{F}_q^*$.*

Proof Our proof proceeds in a similar way as the proof of Theorem 3.5 in [18]. There is $\eta_m \in L_m$ such that $U(L_m/K_m) = \mathbb{F}_q^* \times \langle \eta_m, \sigma(\eta_m) \rangle$, so

$$E(L_m/K_m) := U(L_m/K_m)/\mathbb{F}_q^* \simeq \mathbb{Z}[\sigma]/\langle \sigma^2 + 1 \rangle \simeq \mathbb{Z}[i]$$

https://doi.org/10.4153/CJM-2016-038-2 Published online by Cambridge University Press

as $\mathbb{Z}[\sigma]$-modules. Thus there are $\beta \in \mathbb{Z}[i]$ and $c \in \mathbb{F}_q^*$ such that $\alpha_m = c\eta_m^{\beta}$. Moreover, $E(\alpha_m) := \langle \alpha_m, \sigma(\alpha_m)\rangle \simeq \beta\mathbb{Z}[i]$ as $\mathbb{Z}[\sigma]$-modules.

Thus $[E(L_m/K_m) : E(\alpha_m)] = [\mathbb{Z}[i] : \beta\mathbb{Z}[i]] = N_{\mathbb{Q}(i)/\mathbb{Q}}(\beta)$. From Proposition 3.1, we know that $[E(L_m/K_m) : E(\alpha_m)] \le 2$. If we assume that

$$[E(L_m/K_m) : E(\alpha_m)] = N(\beta) = 2,$$

then $(1-i)$ divides β in $\mathbb{Z}[i]$. Thus, for an element $\tau_m \in E(L_m/K_m)$, we have that for $c \in \mathbb{F}_q^*$, $\alpha_m = c\tau_m^{(1-\sigma)}$. Now we consider a prime p_m of k which is totally ramified in L_m. In other words, $\wp_m^4 = p_m$ for a prime $\wp_m$ of L_m. Since

$$\sigma^i(\tau_m) \equiv \tau_m \text{ in } \mathcal{O}_{L_m}/\wp_m \quad (i = 0, 1, 2, 3),$$

for $c \in \mathbb{F}_q^*$, we have $\sigma^i(\alpha_m) \equiv c$ in $\mathcal{O}_{L_m}/\wp_m$, $(i = 0, 1, 2, 3)$, where $\mathcal{O}_{L_m}$ is the maximal order of L_m. Thus we have that for $c \in \mathbb{F}_q^*$,

$$x^4 - mx^3 - 6x^2 + mx + 1 \equiv (x-c)^4 \text{ in } \mathcal{O}_{L_m}/\wp_m.$$

This implies that for $c \in \mathbb{F}_q^*$, $c^2 \equiv -1$ in $\mathcal{O}_{L_m}/\wp_m$. Since c is an element in $\mathbb{F}_q^*$, $c^2 \equiv -1$ in $\mathcal{O}_{L_m}/\wp_m$ implies that -1 is a square in $\mathbb{F}_q$. Thus, we find that if -1 is not a square in $\mathbb{F}_q$, then $[E(L_m/K_m) : E(\alpha_m)] = 1$. Moreover, we note that -1 is not a square in $\mathbb{F}_q$ if and only if $q \equiv 3 \pmod 4$. This completes the proof. ∎

4 Proof of the Main Result

In this section, we first compute Q_{L_m} and then complete the proof of Theorem 1.1. For this we need the following three lemmas. Gras [4] found the method to determine Q_{L_m} in the number field case, and we develop its function field analogue in this section.

Lemma 4.1 *$Q_{L_m} = 2$ if and only if $N_{L_m/K_m}(U(L_m)) = U(K_m)$, where N_{L_m/K_m} denotes the norm map from L_m to K_m.*

Proof We consider a map $\phi\colon U(L_m) \to U(K_m)/U(K_m)^2$, which is the composition of two maps $N_{L_m/K_m}\colon U(L_m) \to U(K_m)$ and the canonical map $\pi\colon U(K_m) \to U(K_m)/U(K_m)^2$. Then we have $\ker\phi = U(L_m/K_m)U(K_m)$. Thus

$$[U(L_m) : U(K_m)U(L_m/K_m)] \mid [U(K_m) : U(K_m)^2] = 2.$$

Moreover, if $N_{L_m/K_m}(U(L_m)) = U(K_m)$, then ϕ is surjective. Thus, in this case we have $[U(L_m) : U(K_m)U(L_m/K_m)] = [U(K_m) : U(K_m)^2] = 2$. ∎

The following lemma is a criterion to determine if Q_{L_m} is 2. A similar criterion in the number field case is given in [4].

Lemma 4.2 *Let $U(K_m) = \mathbb{F}_q^* \times \langle \epsilon_m\rangle$ and $U(L_m/K_m) = \mathbb{F}_q^* \times \langle \eta_m, \sigma(\eta_m)\rangle$. If $\epsilon_m\eta_m^{1-\sigma}$ is a square in $U(L_m)$ up to a constant in $\mathbb{F}_q^*$, then $Q_{L_m} = 2$.*

Proof Since $\epsilon_m^{1+\sigma}, \eta_m^{-1-\sigma^2} \in \mathbb{F}_q^*$, $u^2 = c\epsilon_m\eta_m^{1-\sigma}$, $(c \in \mathbb{F}_q^*)$ implies that

$$u^{2(1+\sigma)} = c\epsilon_m^{1+\sigma}\eta_m^{1-\sigma^2} = c'\eta_m^2 \quad (c', c \in \mathbb{F}_q^*).$$

https://doi.org/10.4153/CJM-2016-038-2 Published online by Cambridge University Press

Thus $\eta_m = c_1 u_m^{1+\sigma}, \epsilon_m = c_2 u_m^{1+\sigma^2}$, for $(c_1, c_2 \in \mathbb{F}_q^*)$. This implies that $\epsilon_m = c_3 N_{L_m/K_m}(u)$ for $u \in U(L_m)$ and $c_3 \in \mathbb{F}_q^*$. Hence from Lemma 4.1 we can conclude that $Q_{L_m} = 2$. ∎

We first show that $\epsilon_m \eta_m^{1-\sigma}$ is a square in $U(L_m)$ up to a constant in $\mathbb{F}_q^*$. Then we have by Lemma 4.2 that $Q_{L_m} = 2$. It follows that $R(L_m) = (\deg m)^3$. It is thus enough to show that $\epsilon_m \eta_m^{1-\sigma}$ is a square in $U(L_m)$ up to a constant in $\mathbb{F}_q^*$. To check if $\epsilon_m \eta_m^{1-\sigma}$ is a square in $U(L_m)$ up to a constant in $\mathbb{F}_q^*$, we need the following lemma.

Lemma 4.3 *Let E be a quadratic extension of F and $\tau \in E$. If $N_{E/F}(\tau)$ is a square in F and $\mathrm{Tr}_{E/F}(\tau) + 2\sqrt{N_{E/F}(\tau)}$ or $\mathrm{Tr}_{E/F}(\tau) - 2\sqrt{N_{E/F}(\tau)}$ is a square up to a constant of $\mathbb{F}_q^*$ in F, then τ is a square in E up to a constant in $\mathbb{F}_q^*$.*

Proof Suppose that $N_{E/F}(\tau) = w^2$, $\mathrm{Tr}_{E/F}(\tau) + 2\sqrt{N_{E/F}(\tau)} = au^2$ for $a \in \mathbb{F}_q^*$, and $u, w \in E$. Then we can see that

$$N_{E/F}(a\tau) = a^2 N_{E/F}(\tau) = (aw)^2,$$
$$\mathrm{Tr}_{E/F}(a\tau) + 2\sqrt{N_{E/F}(a\tau)} = (au)^2.$$

From [14, Proposition 3.1], we have

$$\sqrt{a\tau} = \frac{a\tau + \sqrt{N_{E/F}(a\tau)}}{\sqrt{\mathrm{Tr}_{E/F}(a\tau) + 2\sqrt{N_{E/F}(a\tau)}}}.$$

It thus follows that τ is square in E up to a constant in $\mathbb{F}_q^*$. Similarly, we can prove the same conclusion in the latter case that $N_{E/F}(\tau)$ and $\mathrm{Tr}_{E/F}(\tau) - 2\sqrt{N_{E/F}(\tau)}$ are square in F. ∎

Proof of Theorem 1.1 In Theorem 3.2 and Theorem 3.3, we find that if $\deg m$ is an odd prime or $q \equiv 3 \pmod 4$, then $\eta_m = c\alpha_m$ for $c \in \mathbb{F}_q^*$. Thus we have $\tau_m := \epsilon_m \eta_m / \sigma(\eta_m) = \epsilon_m \alpha_m / \sigma(\alpha_m)$. We note that

$$N_{L_m/K_m}(\tau_m) = \epsilon_m^2,$$
$$\mathrm{Tr}_{L_m/K_m}(\tau_m) + 2\sqrt{N_{L_m/K_m}(\tau_m)} = \epsilon_m(4 + \sqrt{m^2+16}),$$
$$\mathrm{Tr}_{L_m/K_m}(\tau_m) - 2\sqrt{N_{L_m/K_m}(\tau_m)} = \epsilon_m(\sqrt{m^2+16}).$$

We note that one of

$$\mathrm{Tr}_{L_m/K_m}(\tau_m) + 2\sqrt{N_{L_m/K_m}(\tau_m)} \quad \text{and} \quad \mathrm{Tr}_{L_m/K_m}(\tau_m) - 2\sqrt{N_{L_m/K_m}(\tau_m)}$$

is given by $\epsilon_m(4 + \sqrt{m^2+16}) \in K_m$. Moreover, $\delta_m := \epsilon_m(4 + \sqrt{m^2+16}) \in K_m$ is square in K_m if either $\mathrm{Tr}_{K_m/k}(\delta_m) + 2\sqrt{N_{K_m/k}(\delta_m)}$ or $\mathrm{Tr}_{K_m/k}(\delta_m) - 2\sqrt{N_{K_m/k}(\delta_m)}$ is square in k. We note that

$$N_{K_m/k}(\delta_m) = 16m^2,$$
$$\mathrm{Tr}_{K_m/k}(\delta_m) + 2\sqrt{N_{K_m/k}(\delta_m)} = (2m^2 + 8m + 32 + 8m),$$
$$\mathrm{Tr}_{K_m/k}(\delta_m) - 2\sqrt{N_{K_m/k}(\delta_m)} = (2m^2 + 8m + 32 - 8m).$$

https://doi.org/10.4153/CJM-2016-038-2 Published online by Cambridge University Press

Either $\mathrm{Tr}_{K_m/k}(\delta_m) + 2\sqrt{N_{K_m/k}(\delta_m)}$ or $\mathrm{Tr}_{K_m/k}(\delta_m) - 2\sqrt{N_{K_m/k}(\delta_m)}$ is $2(m+4)^2$. Hence, from Lemma 4.3, we have that δ_m is a square in K_m up to a constant in $\mathbb{F}_q^*$ and τ_m is a square in L_m up to a constant in $\mathbb{F}_q^*$. This completes the proof. ∎

5 Infinitely Many Families of Quartic Function Fields

In this section, we show that there are infinitely many primes q such that $h(t)^2+16$ is square free in $\mathbb{F}_q[t]$, where $h(t)$ is a given monic polynomial in $\mathbb{Z}[t]$. Consequently, Theorem 1.1 holds for infinitely many families of the simplest quartic function fields.

Proposition 5.1 (i) *Let $h(t)$ be of the type $t^k+c \in \mathbb{F}_q[t]$ with $c \in \mathbb{F}_q^*$. Then $h(t)^2+16$ is square free in $\mathbb{F}_q[t]$ for all but finitely many primes q.*

(ii) *Let $h(t) = t^k + at^{k-1} \in \mathbb{Z}[t]$ and $\alpha := -\frac{a(k-1)}{k}$. If $h(\alpha)^2+16 \neq 0$, then $\overline{h}(t)^2+16$ is square free in $\mathbb{F}_q[t]$ for all but finitely many primes q.*

Proof (i) We easily find that a nonzero polynomial $f(t) \in \mathbb{Q}[t]$ is square free if and only if $f(t)$ is relatively prime to $f'(t)$ in $\mathbb{Q}[t]$. Since $h(t)^2+16 = (t^k+c)^2+16$ and $2h(t)h'(t) = 2k(t^k+c)t^{k-1}$ are relatively prime in $\mathbb{Q}[t]$, $h(t)^2+16$ is square free in $\mathbb{Q}[t]$. Now we claim that for $f(t), g(t) \in \mathbb{Z}[t]$, if $f(g(t))$ is square free in $\mathbb{Q}[t]$, then $\overline{f}(\overline{g}(t)) \in \mathbb{F}_q[t]$ is square free for all but finitely many prime q, where $\overline{\alpha}$ denotes the reduction of coefficients of $\alpha \in \mathbb{Z}[t]$ modulo q. If $f(g(t))$ is square free in $\mathbb{Q}[t]$, then $f(g(t))$ and $f(g(t))'$ are relatively prime in $\mathbb{Q}[t]$. Hence, there exist $h_1(t)$ and $h_2(t)$ in $\mathbb{Q}[t]$ such that $f(g(t))h_1(t) + f(g(t))'h_2(t) = 1$. Thus for q such that

$$\overline{f}(\overline{g}(t)) \neq 0, \quad \overline{h}_1(t) \neq 0, \quad \overline{f(g(t))'} \neq 0, \quad \overline{h}_2(t) \neq 0, \tag{5.1}$$

we have $\overline{f}(\overline{g}(t))\overline{h}_1(t) + \overline{f(g(t))'}\overline{h}_2(t) = 1$. Equivalently, $\overline{f}(\overline{g}(t))$ and $\overline{f(g(t))'}$ are relatively prime. Since there are finitely many primes q that do not satisfy the condition of (5.1), it thus follows that $\overline{f}(\overline{g}(t))$ is squarefree in $\mathbb{F}_q[t]$ for all but finitely many primes q. Consequently, we obtain the result.

(ii) We proceed in the same way as (i). We note that $h'(t) = kat^{k-1}(t-\alpha)$. Thus, $h(\alpha)^2+16 \neq 0$ implies that $h(t)^2+16$ is relatively prime to $2h(t)h'(t)$ in $\mathbb{Q}[t]$; so $h(t)^2+16$ is square free in $\mathbb{Q}[t]$. The result thus follows. ∎

Remark 5.2 In Proposition 5.1, we find infinitely many m and q such that m^2+16 is square free in $\mathbb{F}_q[t]$. Moreover, Table 1 and Table 2 in the appendix present a list of m and q satisfying our conditions to determine $R(L_m)$.

6 A Lower Bound of Class Numbers of our Family and Determination of Small Class Numbers

Let $R(K)$ be the regulator of K, $h(K)$ the *divisor class number* (that is, the number of divisor classes of degree zero of K), and $h'(K)$ the ideal class number of K (that is, the number of ideal classes of the maximal ideal $\mathcal{O}_K$ of K), simply a so-called *class number* of K throughout this paper. Then we have that $h(K) = R(K)h'(K)$.

https://doi.org/10.4153/CJM-2016-038-2 Published online by Cambridge University Press

Lemma 6.1 (Weil Theorem) *Let K be a global function field whose constant field $\mathbb{F}$ has q elements. Let $N_1(K)$ denote the number of prime divisors of degree 1 of K and let g_K be the genus of K. Then $|N_1(K) - q - 1| \le 2g_K\sqrt{q}$.*

Proof See [16, Proposition 5.11]. ∎

Let K be a function field over $\mathbb{F}_q$ and $\widetilde{K}$ be the constant field extension of K with an extension degree n. Since $g_{\widetilde{K}} = g_K$, we have

$$N_1(\widetilde{K}) \ge q^n + 1 - 2g_K\sqrt{q^n}. \tag{6.1}$$

Lemma 6.2 *Let K be a function field over $\mathbb{F}_q$ and $\widetilde{K}$ be the constant field extension of K with an extension degree n. Let P be a prime divisor of K. If $\deg_K(P)$ divides n, then P splits into $\deg_K(P)$ primes of degree 1 in $\widetilde{K}$.*

Proof See [16, Proposition 8.13]. ∎

We thus can see that the number of integral divisors of degree n in K is at least $N_1(\widetilde{K})/n$.

Lemma 6.3 (Riemann–Roch Theorem) *The dimension $d(C)$ of a divisor class C of degree $2g_K - 1$ in K is $d(C) = \deg C + 1 - g_K$.*

Lemma 6.4 *The genus g_{L_m} of L_m is given by $g_{L_m} = 3(\deg m - 1)$.*

Proof Since the infinite prime in k splits completely in L_m, we obtain the result due to the Hurwitz genus formula. ∎

In the following theorem, we obtain a lower bound of the divisor class numbers of $\{L_m\}$; cases of quadratic function fields have been treated in [3, Theorem 4.1].

Theorem 6.5 *If $\deg m > 1$, then the divisor class number $h(L_m)$ of L_m has a lower bound given by*

$$h(L_m) \ge \frac{q-1}{q^{g_{L_m}} - 1} \frac{q^{2g_{L_m}-1} + 1 - 2g_{L_m} q^{\frac{2g_{L_m}-1}{2}}}{2g_{L_m} - 1}.$$

Moreover, if $\deg m = 1$, then $h(L_m) = 1$.

Proof If $\deg m = 1$, then the genus of L_m is 0 by Lemma 6.4, and so the divisor class number of L_m is 1.

Now we consider the case when $\deg m > 1$. Let $n = 2g_{L_m} - 1$. Then the number of divisor classes of degree n is $h(L_m)$, and there are $(q^{d(C)} - 1)/(q-1)$ integral divisors in each class C. Thus the number of integral divisors in L_m is $h(L_m)(q^{d(C)} - 1)/(q-1)$ and it is greater than or equal to $\frac{N_1(\widetilde{L}_m)}{n}$, where $\widetilde{L}_m$ is a constant extension of L_m of an extension degree n. It thus follows from (6.1) that

$$h(L_m)\frac{q^{d(C)} - 1}{q-1} \ge \frac{N_1(\widetilde{L}_m)}{n} \ge \frac{q^n + 1 - 2g_{L_m} q^{\frac{n}{2}}}{n}.$$ ∎

https://doi.org/10.4153/CJM-2016-038-2 Published online by Cambridge University Press

Theorem 6.6 *If* $\deg m > 1$*, then the ideal class number* $h'(L_m)$ *of* L_m *has a lower bound given by*

$$h'(L_m) \geq \frac{1}{2(\deg m)^3}\frac{q-1}{q^{3(\deg m-1)}-1}\frac{q^{6(\deg m)-7}+1-6(\deg m-1)q^{\frac{6(\deg m)-7}{2}}}{6(\deg m)-7}.$$

Moreover, if $\deg m = 1$*, then* $h'(L_m) = 1$*.*

Proof We note that

$$n = 2g_{L_m} - 1 = 6(\deg m) - 7 \quad \text{and} \quad d(C) = g_{L_m} = 3(\deg m - 1).$$

From Proposition 3.1, we have $R(L_m) \leq 2(\deg m)^3$. Thus we obtain the result from Theorem 6.5. ∎

Corollary 6.7 *If* $h'(L_m) \leq 20$*, then either* $\deg m = 1$ *or* $q \leq 11$ *and* $\deg m \leq 4$*. Moreover, the list in Table 3 is a complete list of q and m for which the class numbers of* L_m *are less than or equal to* 20*, where* $\deg m > 1$*, and the class number computation is made by Magma.*

7 Contribution to Computing Divisor Class Numbers of Cyclic Quartic Function Fields

Let $L_{L_m}(u) = \prod_{j=1}^{g}(1-\omega_j u)$, where g is the genus of L_m. Then it is known that $h(L_m) = L_{L_m}(1) = q^g L_{L_m}(1/q)$. For $u = q^s$, we have $L_{L_m}(u) = (1-u)(1-qu)\zeta_{L_m}(s)$, where $\zeta_{L_m}(s) = \sum_{\mathfrak{a}\geq 0} N(\mathfrak{a})^{-s} = \prod_{\nu=1}^{\infty}\prod_{\deg(\mathfrak{p})=\nu}\frac{1}{1-u^{\nu}}$.

We note that

$$\zeta_{L_m}(s) = \prod_{\nu=1}^{\infty}\prod_{\deg(\mathfrak{p})=\nu}\frac{1}{1-u^{\nu}} = \zeta_{L_m}^{\infty}(u)\zeta_{L_m}^{x}(u).$$

Since an infinite prime on L_m splits completely in L_m, we have $\zeta_{L_m}^{\infty}(u) = \frac{1}{(1-u)^4}$. Moreover, for a monic irreducible $p \in \mathbb{F}_q[t]$,

$$\zeta_{L_m}^{x}(u) = \prod_{\nu=1}^{\infty}\prod_{\deg p=\nu}\prod_{\mathfrak{p}|p}\frac{1}{1-u^{\deg\mathfrak{p}}}.$$

We note that for a monic irreducible $p \in \mathbb{F}_q[t]$ with $\deg p = \nu$ and $\mathfrak{p} \mid p$,

$$\prod_{\mathfrak{p}|p}\frac{1}{1-u^{\deg\mathfrak{p}}} = \begin{cases}(1-u^{\nu})^{-4} & \text{if } (e(p),f(p),g(p)) = (1,1,4),\\ (1-u^{2\nu})^{-2} & \text{if } (e(p),f(p),g(p)) = (1,2,2),\\ (1-u^{\nu})^{-1} & \text{if } (e(p),f(p),g(p)) = (4,1,1),\\ (1-u^{4\nu})^{-1} & \text{if } (e(p),f(p),g(p)) = (1,4,1),\end{cases}$$

where for the extension of L_m over k, $e(p)$ is the ramification index of the prime ideal (p), $f(p)$ is the residue class field degree of (p), and $g(p)$ is the number of the primes of L_m lying above (p).

https://doi.org/10.4153/CJM-2016-038-2 Published online by Cambridge University Press

Thus by defining

$$Z_i(p) := \begin{cases} 1 & \text{if } (e(p), f(p), g(p)) = (1,1,4), \\ (-1)^i & \text{if } (e(p), f(p), g(p)) = (1,2,2), \\ 0 & \text{if } (e(p), f(p), g(p)) = (4,1,1), \\ \zeta_4^i & \text{if } (e(p), f(p), g(p)) = (1,4,1), \end{cases}$$

we can rewrite

$$\zeta_{L_m}^x(u) = \prod_{\nu=1}^{\infty} \prod_{\deg p=\nu} (1-u^\nu)^{-1} \prod_{i=1}^{3} (1 - Z_i(p)u^\nu)^{-1}.$$

We define $S_\nu(\ell) := \sum_{\deg p=\nu} \sum_{j=1}^{3} Z_i(p)^\ell$. Since

$$\prod_{\nu=1}^{\infty} \prod_{\deg p=\nu} (1-u^\nu)^{-1} = (1-qu)^{-1},$$

we can rewrite

$$\log h(L_m) = g \log q - 3\log\Big(1 - \frac{1}{q}\Big) + \sum_{\ell=1}^{\infty} \frac{1}{\ell q^\ell} \sum_{\nu \mid \ell} S_\nu\Big(\frac{\ell}{\nu}\Big).$$

Thus, we have $h(L_m) = E(\lambda)e^{B(\lambda)}$, where

$$\log E(\lambda) = g \log q - 3\Big(1 - \frac{1}{q}\Big) + \sum_{\ell=1}^{\lambda} \frac{1}{\ell q^\ell} \sum_{\nu \mid \ell} S_\nu\Big(\frac{\ell}{\nu}\Big),$$

$$B(\lambda) = \sum_{\ell \geq \lambda} \frac{1}{\ell q^\ell} \sum_{\nu \mid \ell} S_\nu\Big(\frac{\ell}{\nu}\Big),$$

and $|h(L_m) - E(\lambda)| \leq |E(\lambda)||(e^{B(\lambda)} - 1)|$. Moreover, we have that

$$E(\lambda) < e^{g \log q - 3\log(1-\frac{1}{q})} \Big(\frac{\sqrt{q}}{\sqrt{q}-1}\Big)^{2g} \Big(\frac{q}{q-1}\Big)^3,$$

$$B(\lambda) < \frac{2g}{\lambda+1} q^{-\frac{\lambda+1}{2}} + \frac{2g}{\lambda+2} \frac{\sqrt{q}}{\sqrt{q}-1} q^{-\frac{\lambda+2}{2}} + \frac{3}{\lambda+1} \frac{q}{q-1} q^{-\lambda+1}$$

(see [17]).

Computation of $E(\lambda)$ To compute $E(\lambda)$, we need to calculate $S_\nu(\ell)$. In the following, we represent $S_\nu(\ell)$ by using the number of primes p of k with a given *signature* $(e(p), f(p), g(p))$ in L_m. We define $N_i(\nu)$ as follows: $N_i(\nu)$:= the number of primes p with degree ν such that

$$(e(p), f(p), g(p)) = \begin{cases} (1,1,4) & \text{if } i = 1, \\ (1,2,2) & \text{if } i = 2, \\ (4,1,1) & \text{if } i = 3, \\ (1,4,1) & \text{if } i = 4. \end{cases}$$

Then we have the following theorem.

https://doi.org/10.4153/CJM-2016-038-2 Published online by Cambridge University Press

Theorem 7.1

$$S_v(\ell) = \begin{cases} 3(N_1(v)+N_2(v)+N_4(v)) & \text{if } \ell \equiv 0 \pmod 4, \\ 3N_1(v)-(N_2(v)+N_4(v)) & \text{if } \ell \equiv 1 \pmod 4, \\ 3(N_1(v)+N_2(v))-N_4(v) & \text{if } \ell \equiv 2 \pmod 4, \\ 3N_1(v)-(N_2(v)+N_4(v)) & \text{if } \ell \equiv 3 \pmod 4. \end{cases}$$

Proof By the definitions of $N_i(v)$, $S_v(\ell)$, and $Z_i(p)$, we can obtain the result by simple computation. ∎

We can find an explicit criterion for characterization of signature types of all the primes of k in $\{L_m\}$ since $S_v(\ell)$ is explicitly determined by signature types of all the primes of k in $\{L_m\}$.

Theorem 7.2 *Signature types of all the primes of k in $\{L_m\}$ are explicitly determined as follows:*

$$(e(p), f(p), g(p)) = \begin{cases} (1,1,4) & \text{if } \Delta_m \not\equiv 0 \pmod p, \left(\frac{\Delta_m}{p}\right)=1, \left(\frac{\Delta_m - m\sqrt{\Delta_m}}{p}\right)=1, \\ (1,2,2) & \text{if } \Delta_m \not\equiv 0 \pmod p, \left(\frac{\Delta_m}{p}\right)=1, \left(\frac{\Delta_m - m\sqrt{\Delta_m}}{p}\right)\neq 1, \\ (4,1,1) & \text{if } m \equiv 0 \pmod p, \Delta_m \equiv 0 \pmod p, \\ (1,4,1) & \text{if } \Delta_m \not\equiv 0 \pmod p, \left(\frac{\Delta_m}{p}\right)\neq 1, \end{cases}$$

where $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol.

Proof We have

$$x^4 - mx^3 - 6x^2 + mx + 1 = (x-\alpha_{1,m})(x-\alpha_{2,m})(x-\alpha_{3,m})(x-\alpha_{4,m})$$

with

$$\alpha_{1,m} = \frac{1}{2}\left(\frac{m+\sqrt{\Delta_m}}{2} + \sqrt{\frac{\Delta_m + m\sqrt{\Delta_m}}{2}}\right),$$

$$\alpha_{2,m} = \frac{1}{2}\left(\frac{m-\sqrt{\Delta_m}}{2} + \sqrt{\frac{\Delta_m - m\sqrt{\Delta_m}}{2}}\right),$$

$$\alpha_{3,m} = \frac{1}{2}\left(\frac{m+\sqrt{\Delta_m}}{2} - \sqrt{\frac{\Delta_m + m\sqrt{\Delta_m}}{2}}\right),$$

$$\alpha_{4,m} = \frac{1}{2}\left(\frac{m-\sqrt{\Delta_m}}{2} - \sqrt{\frac{\Delta_m - m\sqrt{\Delta_m}}{2}}\right).$$

The result thus follows immediately. ∎

Complexity of Computation of $E(\lambda)$ See [17, 4.1].

Let $t(\lambda)$ be the time required for computing $E(\lambda)$. For computing $E(\lambda)$, we need to calculate $S_v(i)$ for $v \leq \lambda$. We can represent $S_v(i)$ using the number of primes in k with a given signature type. Thus $t(\lambda)$ is approximately the product of the number of irreducible polynomials and the running time T to determine the signature type of the principal ideal $(p(t))$ for an irreducible polynomial $p(t) \in \mathbb{F}_q[t]$. Therefore, the

https://doi.org/10.4153/CJM-2016-038-2 Published online by Cambridge University Press

complexity of computation of $E(\lambda)$ is given by $O(\frac{q^\lambda}{\lambda}T)$. We note that the complexity of computation of $E(\lambda)$ depends on λ. If we have the exact value of the regulator $R(K)$, then we can possibly obtain a more efficient algorithm for computing the divisor class number $h(L_m)$ of L_m by the reduction of $E(\lambda)$. We discuss more details below.

Using the upper bound of $E(\lambda)$ and $B(\lambda)$, we can compute the error term of $h(L_m) - E(\lambda)$. The fact that $h(L_m)$ is an integer is importantly used for finding the truncated point of λ to make the error term

$$|E(\lambda)(e^{B(\lambda)} - 1)| < 1/2. \tag{7.1}$$

Since $h(L_m)$ is a multiple of $R(L_m)$, if we know the exact value of $R(L_m)$, then the truncated point of λ is the smallest integer satisfying

$$|E(\lambda)(e^{B(\lambda)} - 1)| < R(L_m)/2. \tag{7.2}$$

Since $E(\lambda)e^{B(\lambda)} - 1$ is a decreasing function on λ, the smallest integer satisfying (7.2) is much smaller than the smallest integer satisfying (7.1).

8 Divisibility of Divisor Class Numbers of Cyclotomic Function Fields

In this section, we study the divisibility of the divisor class numbers of cyclotomic function fields which contain $\{L_m\}$ as their subfields.

Let E be a finite abelian extension of k. Then the *conductor* of E is the monic polynomial $N \in \mathbb{F}_q[t]$ such that $k(\Lambda_N)$ is the smallest cyclotomic function field containing E. Recall that the cyclotomic function field $k(\Lambda_N)$ is defined via the Carlitz module [16, Chapter 12].

If $m^2 + 16$ is square free in $\mathbb{F}_q[t]$ for $m \in \mathbb{F}_q[t]$, then the discriminant $D(K_m)$ (respectively, $D(L_m)$) of K_m (respectively, L_m) over k is $m^2 + 16$ (respectively, $(m^2+16)^3$). Since L_m is a cyclic extension of k with the unique quadratic subfield K_m, the conductor $f(L_m/k)$ of L_m over k is equal to

$$f(L_m/k) = (D(L_m)/D(K_m))^{\frac{1}{2}} = m^2 + 16$$

[7, Corollary on p. 332]. It thus follows that L_m is a subfield of the cyclotomic function field $k(\Lambda_{m^2+16})$.

We note that for a monic polynomial $m \in \mathbb{F}_q[t]$, we have

$$L_m = k\left(\sqrt{\frac{m^2+16+m\sqrt{m^2+16}}{2}}\right).$$

Moreover, for $m = t^d + a_{d-1}t^{d-1} + \cdots + a_0 \in \mathbb{F}_q[t]$ and $u = t^{-1}$,

$$\sqrt{\frac{m^2+16+m\sqrt{m^2+16}}{2}} = u^{-d} + b_{-(d-1)}u^{-(d-1)} + b_{-(d-2)}u^{-(d-2)} + \cdots \in \mathbb{F}_q((u)).$$

Since $u = 1/t$ is a local parameter of the infinite prime $\wp_\infty$ of k, $\wp_\infty$ splits completely in L_m and L_m is a subfield of the maximal real subfield $k(\Lambda_{m^2+16})^+$ of the cyclotomic function field $k(\Lambda_{m^2+16})$. Then the divisor class number $h(k(\Lambda_{m^2+16})^+)$ is divisible

https://doi.org/10.4153/CJM-2016-038-2 Published online by Cambridge University Press

by the divisor class number $h(L_m)$ as $k(\Lambda_{m^2+16})^+$ is a geometric extension of L_m [16, Corollary 1, p. 252]. We therefore obtain the following result.

Theorem 8.1 *Let $m \in \mathbb{F}_q[t]$ be such that $m^2 + 16$ is square free in $\mathbb{F}_q[t]$ and $q \equiv 3 \pmod 4$. Let $k(\Lambda_{m^2+16})^+$ be the maximal real subfield of the cyclotomic function field $k(\Lambda_{m^2+16})$. Then we have the following divisibility of the divisor class number $h(k(\Lambda_{m^2+16})^+)$:*

$$(\deg m)^3 \mid h(k(\Lambda_{m^2+16})^+).$$

We thus observe the following. For a given positive integer a and all but finitely many primes q with $q \equiv 3 \pmod 4$, there are infinitely many $m \in \mathbb{F}_q[t]$ such that the divisor class number $h(k(\Lambda_{m^2+16})^+)$ is divisible by a^3.

Proof The first assertion follows immediately from Theorem 1.1. For the second assertion, let a be a given positive integer. Let $m := m_d = t^{ad} + c$ for a positive integer d and $c \in \mathbb{F}_q$. Then $m^2 + 16$ is square free in $\mathbb{F}_q[t]$ for all but finitely many q by Proposition 5.1. From Theorem 1.1, we find that if $q \equiv 3 \pmod 4$, then the regulator $R(L_m)$ of L_m is $(\deg m)^3$. Therefore, the divisor class number $h(L_m)$ is divisible by the regulator $R(L_m) = (\deg m)^3 = d^3a^3$, and so the divisor class number $h(k(\Lambda_{m^2+16})^+)$ is divisible by a^3 because it is divisible by the divisor class number $h(L_m)$. This holds for the infinite family of $m = t^{ad} + c$ with any positive integer d. The result thus follows as desired. ■

According to [6, Theorem 3.4], there is a lower bound on the p-part of $h(k(\Lambda_{Q^n})^+)$ under the condition that p divides $h(k(\Lambda_Q)^+)$, where p is the characteristic of k and Q is an irreducible polynomial in k. As in the proof of Theorem 8.1, we can explicitly find irreducible polynomials Q with $p \mid h(k(\Lambda_Q)^+)$. By combining Theorem 8.1 with [6, Theorem 3.4], we thus obtain the following result.

Proposition 8.2 *Let p be a prime with $p \equiv 3 \pmod 4$ and m be a monic polynomial in $\mathbb{F}_p[t]$ such that $m^2 + 16$ is irreducible in $\mathbb{F}_p[t]$ with $p \mid \deg m$. Then for any positive integer n, we have $p^{e(n)} \mid h(k(\Lambda_{(m^2+16)^n})^+)$, where*

$$e(n) := \Big[\frac{p^{(n-1)2\deg m} - 1}{n(p-1)}\Big]$$

and $[x]$ denotes the greatest integer that is less than or equal to x.

Remark 8.3 From Proposition 8.2, we can find irreducible polynomials $Q \in \mathbb{F}_p[t]$ such that the exponent of the p-part of $h(k(\Lambda_{Q^n})^+)$ is at least

$$\Big[\frac{p^{(n-1)2\deg m} - 1}{n(p-1)}\Big].$$

For example, in the case when $p = 3$, we have that if $m = t^3 + t$, $t^3 + t^2$, or $t^3 + 2t^2$, then $m^2 + 16$ is an irreducible polynomial in $\mathbb{F}_3[t]$. Thus for such m, we obtain that

$$3^{[\frac{3^{(n-1)6}-1}{2n}]} \mid h(k(\Lambda_{(m^2+16)^n})^+).$$

https://doi.org/10.4153/CJM-2016-038-2 Published online by Cambridge University Press

Moreover, we see that if $m = t^6 + t^4 + 2t^2 + t$, $t^6 + t^5 + 2t^2 + t$, or $t^6 + t^4 + 2t^2 + 2t$, then $m^2 + 16$ is an irreducible polynomial in $\mathbb{F}_3[t]$. Consequently, for such m, it follows that

$$3^{[\frac{3(n-1)12-1}{2n}]} \mid h(k(\Lambda_{(m^2+16)^n})^+).$$

Appendix

Using Theorem 1.1 and Proposition 5.1, we find Table 1, which is a list of regulators of L_m, where $\deg m$ is an odd prime, for all but finitely many primes q.

Table 1: Regulators of L_m, where $\deg m$ is an odd prime

m	$R(L_m)$	m	$R(L_m)$
t^3	3^3	$t^3 + 3t^2 + 2$	3^3
t^5	5^3	$t^5 + 3t^4 + 2t^3 + 2t$	5^3
t^7	7^3	$t^7 + 3t^6 + 2t^5 + 8t^4 + 4t^3 + 2t$	7^3
t^{11}	11^3	$t^{11} + 3t^{10} + 2t^9 + 8t^5 + 4t^3 + 2t$	11^3
t^{13}	13^3	$t^{13} + t^{12} + t^6 + 5t^3 + 4t + 1$	13^3
t^{17}	17^3	$t^{17} + t^{12} + t^6 + 5t^3 + 4t + 1$	17^3
t^{19}	19^3	$t^{19} + t^{12} + t^6 + 5t^3 + 4t + 1$	19^3
t^{23}	23^3	$t^{23} + 3t^{10} + t^9$	23^3
t^{29}	29^3	$t^{29} + 3t^{10} + t^9$	29^3

Table 2 is a list of regulators of L_m, where $\deg(m)$ is composite, for all but finitely many primes q with $q \equiv 3 \pmod r$.

Table 2: Regulators of L_m, where $\deg(m)$ is composite and $q \equiv 3 \pmod 4$

m	$R(L_m)$	m	$R(L_m)$
t^{15}	15^3	$t^{15} + t^{12} + 3t^4 + 5$	15^3
t^{21}	21^3	$t^{21} + t^{12} + 3t^4 + 5$	21^3
t^{35}	35^3	$t^{35} + t^{12} + 3t^4 + 5$	35^3
t^{143}	143^3	$t^{143} + t^{120} + 3t^4 + 5$	143^3
t^{187}	187^3	$t^{187} + t^{140} + 3t^4 + 5$	187^3
t^{221}	221^3	$t^{221} + t^{201} + 3t^{94} + 7$	221^3
t^{247}	247^3	$t^{247} + t^{20} + 3t^4 + 5$	247^3
t^{253}	253^3	$t^{253} + t^{220} + 3t^{47} + 5$	253^3
t^{319}	319^3	$t^{319} + 7t^{201} + 3t^4 + 5$	319^3

https://doi.org/10.4153/CJM-2016-038-2 Published online by Cambridge University Press

Table 3: A complete list with ideal class numbers ≤ 20, except the case when deg $m = 1$

$h'(L_m)$	q	m		
1	3	t^3,	t^3+2,	t^3+1
2	5	t^2+3t+3,	t^2+t+2,	t^2+2,
		t^2+t+1,	t^2+3,	t^2+4t+1,
		t^2+2t+4,	t^2+3t+4,	t^2+2t+3,
		t^2+4t+2		
3	3	t^2+2t,	t^2+2,	t^2+t
4	3	t^2+t+1,	t^2,	t^2+2t+1
5	3	t^2+1,	t^2+t+2,	t^2+2t+2
8	5	t^2+4,	t^2+4t+4,	t^2,
		t^2+2t+1,	t^2+3t+1	
13	3	t^3+2t+1,	t^3+2t+2	
16	5	t^2+4,	t^2+2t+2,	t^2+4t+3,
		t^2+1,	t^2+t+3,	t^2+3t,
		t^2+3t+2,	t^2+2t,	t^2+4t,
		t^2+t		
20	3	t^3+t^2+2,	t^3+t^2+t+2,	t^3+t^2+2t+1,
		t^3+2t^2+1,	t^3+2t^2+t+1,	t^3+2t^2+2t+2
20	7	t^2+5t+5,	t^2+6t+6,	t^2+4t+1,
		t^2+2t+5,	t^2+4,	t^2+t+6,
		t^2+3t+1		

Acknowledgment The authors express gratitude to an anonymous referee for very helpful suggestions.

References

[1] S. Bae, *Real quadratic function fields of Richaud-Degert type with ideal class number one*. Proc. Amer. Soc. Math. **140**(2011), no. 2, 403–414. http://dx.doi.org/10.1090/S0002-9939-2011-10910-9

[2] J. W. S. Cassels, *An introduction to the geometry of numbers*. Springer-Verlag, Berlin, 1971.

[3] K. Feng and W. Hu, *On real quadratic function fields of Chowla type with ideal class number one*. Proc. Amer. Soc. Math. **127**(1999), no. 5, 1301–1307. http://dx.doi.org/10.1090/S0002-9939-99-05004-2

[4] M-N. Gras, *Table numérique du nombre de classes et des unités des extensions cycliques réelles de degré 4 de* $\mathbb{Q}$. Publ. Math. Fac. Sci. Besançon, Théorie des Nombres, Fasc. 2, (1977/78) 1–53.

[5] ———, *Special units in real cyclic sextic fields*. Math. Comp. **48**(1987), no. 177, 179–182. http://dx.doi.org/10.1090/S0025-5718-1987-0866107-1

[6] L. Guo and L. Shu, *Class numbers of cyclotomic function fields*. Trans. Amer. Math. Soc. **351**(1999), no. 11, 4445–4467. http://dx.doi.org/10.1090/S0002-9947-99-02325-9

[7] M. Haghighi, *Computation of conductor for finite extensions with cyclic Galois groups*. J. Algebra **124**(1989), no. 2, 329–333. http://dx.doi.org/10.1016/0021-8693(89)90134-8

https://doi.org/10.4153/CJM-2016-038-2 Published online by Cambridge University Press

[8] H. Hasse, Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern, *Mathematische Abhandlungen*. Band 3, Walter de Gruyter, Berlin, 1975, pp. 290–379.

[9] B-H. Im and Y. Lee, *Decomposition of places in dihedral and cyclic quintic trinomial extensions of global fields*. Manuscripta Math. **137**(2012), no. 1-2, 107–127. http://dx.doi.org/10.1007/s00229-011-0459-4

[10] Y. Kishi, *A family of cyclic cubic polynomials whose roots are systems of fundamental units*. J. Number Theory **102**(2003), no. 1, 90–106. http://dx.doi.org/10.1016/S0022-314X(03)00085-4

[11] A. J. Lazarus, *On the class number and unit index of simplest quartic fields*. Nagoya Math. J. **121**(1991), 1–13. http://dx.doi.org/10.1017/S0027763000003378

[12] Y. Lee, R. Scheidler, and C. Yarrish, *Computation of the fundamental units and the regulator of a cyclic cubic function field*. Experiment. Math. **12**(2003), no. 2, 211–225. http://dx.doi.org/10.1080/10586458.2003.10504493

[13] E. Lehmer, *Connection between Gaussian periods and cyclic units*. Math. Comp. **50**(1988), no. 182, 535–541. http://dx.doi.org/10.1090/S0025-5718-1988-0929551-0

[14] S. R. Louboutin, *Hasse unit indices of dihedral octic CM-fields*. Math. Nachr. **215**(2000), 107–113. http://dx.doi.org/10.1002/1522-2616(200007)215:1<107::AID-MANA107>3.0.CO;2-A

[15] ———, *The simplest quartic fields with ideal class groups of exponents less than or equal to 2*. J. Math. Soc. Japan **56**(2004), no. 3, 717–727. http://dx.doi.org/10.2969/jmsj/1191334082

[16] M. Rosen, *Number theory in function fields*. Graduate Texts in Mathematics, 210. Springer-Verlag, New York, 2002. http://dx.doi.org/10.1007/978-1-4757-6046-0,

[17] R. Scheidler and A. Stein, *Approximating Euler products and class number computation in algebraic function fields*. Rocky Mountain J. Math. **40**(2010), no. 5, 1689–1727. http://dx.doi.org/10.1216/RMJ-2010-40-5-1689

[18] R. Schoof and L. C. Washington, *Quintic polynomials and real cyclotomic fields with large class numbers*. Math. Comp. **50**(1988), no. 182, 543–556. http://dx.doi.org/10.2307/2008623

[19] Y. Y. Shen, *Unit groups and class numbers of real cyclic octic fields*. Trans. Amer. Math. Soc. **326**(1991), no. 1, 179–209. http://dx.doi.org/10.1090/S0002-9947-1991-1031243-3

[20] A. Stein and H. C. Williams, *Some methods for evaluating the regulator of a real quadratic function field*. Experiment. Math. **8**(1999), no. 2, 119–133. http://dx.doi.org/10.1080/10586458.1999.10504394

[21] K. Tomita and K. Yamamuro, *Lower bounds for fundamental units of real quadratic fields*. Nagoya Math. J. **166**(2002), 29–37. http://dx.doi.org/10.1017/S0027763000008230

[22] L. C. Washington, *A family of cyclic quartic fields arising from modular curves*. Math. Comp. **57**(1991), no. 196, 763–775. http://dx.doi.org/10.1090/S0025-5718-1991-1094964-6

[23] H. C. Williams and C. R. Zarnke, *Computer calculation of units in cubic fields*. Proceedings of the Second Manitoba Conference on Numerical Mathematics, Congressus Numerantium VII (1972), 433–468.

[24] Q. Wu and R. Scheidler, *An explicit treatment of biquadratic function fields*. Contrib. Discrete Math. **2**(2007), no. 1, 43–60.

[25] Z. Zhang and Q. Yue, *Fundamental units of real quadratic fields of odd class number*. J. Number Theory **137**(2014), 122–129. http://dx.doi.org/10.1016/j.jnt.2013.10.019

Institute of Mathematical Sciences, Ewha Womans University, 52, Ewhayeodae-gil, Seodaemun-gu, Seoul 03760, Republic of Korea
e-mail: lee9311@ewha.ac.kr

Department of Mathematics, Ewha Womans University, 52, Ewhayeodae-gil, Seodaemun-gu, Seoul 03760, Republic of Korea
e-mail: yoonjinl@ewha.ac.kr

https://doi.org/10.4153/CJM-2016-038-2 Published online by Cambridge University Press